



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10241287 A**(43) Date of publication of application: **11.09.98**

(51) Int. Cl.

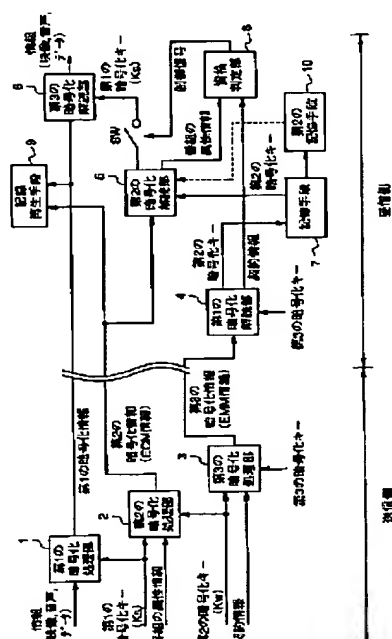
G11B 20/10(21) Application number: **09040529**(22) Date of filing: **25.02.97**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**(72) Inventor: **KUNIHIRA TADASHI**(54) **DIGITAL INFORMATION
RECORDING/REPRODUCING DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To reproduce recorded digital information for a specified period without reducing security by using a digital information ciphering transmission system constructed for deciphering second ciphering information reproduced by a recording/reproducing means by using a second ciphering key held in a first or second storage means.

SOLUTION: The storage means 7 of a digital information recording/ reproducing device receives and holds a second ciphering key outputted from a first cryptoanalysis section 4 and then outputs this to a second cryptoanalysis section 5. The held second ciphering key is also outputted to a second storage means 10 and held there for a fixed period. When a recording/reproducing means 9 reproduces the recorded first or second ciphering information, the second cryptoanalysis section 5 for decoding the second ciphering information decodes the reproduced second ciphering information by using the second ciphering key held in the first or second storage means 7 or 10.

COPYRIGHT: (C)1998,JPO



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-241287

(43)公開日 平成10年(1998) 9月11日

(51)Int.Cl.⁶

G 1 1 B 20/10

識別記号

F I

G 1 1 B 20/10

H

審査請求 未請求 請求項の数 8 O L (全 19 頁)

(21)出願番号 特願平9-40529

(22)出願日 平成9年(1997) 2月25日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 國平 幸司

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

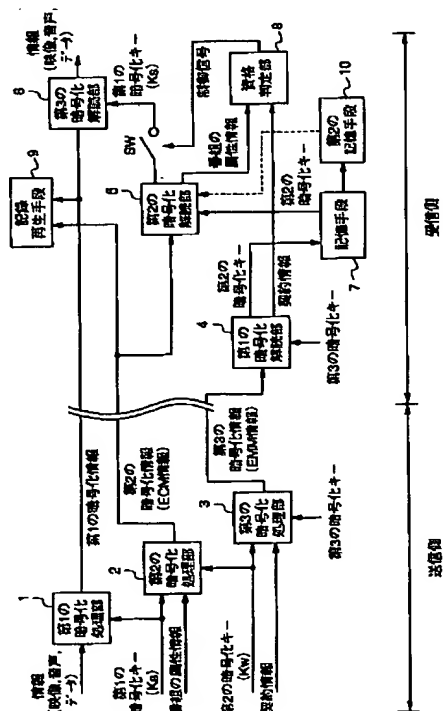
(74)代理人 弁理士 早瀬 憲一

(54)【発明の名称】 デジタル情報記録再生装置

(57)【要約】

【課題】 システムにおけるセキュリティを低下させることなく、所定の期間は、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を得る。

【解決手段】 記憶手段7に保持している第2の暗号化キーを記憶手段7のデータ変更後一定期間保持する第2の記憶手段10を備え、第1、第2の暗号化情報を記録、再生する記録再生手段9が、記録した第1、第2の暗号化情報を再生するときに、第2の暗号化情報（ECM情報）を解読する第2の暗号化解読部が、前記記録再生手段が再生した第2の暗号化情報を、前記第1または第2の記憶手段に保持された第2の暗号化キーを用いて暗号を解除する構成とした。



【特許請求の範囲】

【請求項 1】 放送局より伝送される、情報を第 1 の期間ごとに变化する第 1 の暗号化キーを用いて暗号化した第 1 の暗号化情報、前記第 1 の暗号化キーと前記情報の属性情報を第 2 の期間ごとに变化する第 2 の暗号化キーにより暗号化した第 2 の暗号化情報、及び次の第 2 の期間に有効な第 2 の暗号化キーと個別の契約情報を第 3 の暗号化キーにより暗号化した第 3 の暗号化情報を受信する手段と、

受信した第 3 の暗号化情報を前記第 3 の暗号化キーを用いて暗号を解除して前記第 2 の暗号化キーと前記個別の契約情報を出力する第 1 の暗号化読取部と、

該第 1 の暗号化読取部が出力する第 2 の暗号化キーを次の第 2 の期間の間保持する第 1 の記憶手段と、

受信した第 2 の暗号化情報を、一つ前の第 2 の期間に得られ前記第 1 の記憶手段に保持された第 2 の暗号化キーを用いて暗号を解除して前記第 1 の暗号化キーと前記情報の属性情報を出力する第 2 の暗号化読取部と、

受信した第 1 の暗号化情報を、前記第 2 の暗号化読取部より出力され、前記第 1 の暗号化読取部より出力された個別の契約情報と前記第 2 の暗号化読取部より出力された情報の属性情報との比較に基づいて与えられる、第 1 の暗号化キーを用いて暗号を解除して前記情報を得る第 3 の暗号化読取部と、

受信した第 1、及び第 2 の暗号化情報を記録、再生する記録再生手段と、

前記第 1 の記憶手段に保持している第 2 の暗号化キーを前記第 1 の記憶手段のデータ変更後一定期間保持する第 2 の記憶手段とを備え、

前記記録再生手段に記録された情報の再生時に、前記第 2 の暗号化読取部が、前記記録再生手段が再生した第 2 の暗号化情報を、前記第 1 または第 2 の記憶手段に保持された第 2 の暗号化キーを用いて暗号を解除することを特徴とするデジタル情報記録再生装置。

【請求項 2】 請求項 1 記載のデジタル情報記録再生装置において、

前記記録再生手段は、第 1、第 2 の暗号化情報とともに記録時の時間情報を記録することを特徴とするデジタル情報記録再生装置。

【請求項 3】 請求項 2 記載のデジタル情報記録再生装置において、

前記記録再生手段に記録された第 1、第 2 の暗号化情報を、該第 1、第 2 の暗号化情報が前記記録再生手段に記録された時から上記第 2 の記憶手段が第 2 の暗号化キーを保持する上記一定期間を上限とする所定期間に限り再生可能とする制御手段をさらに備えたことを特徴とするデジタル情報記録再生装置。

【請求項 4】 請求項 1 または請求項 3 記載のデジタル情報記録再生装置において、

前記記録再生手段は、第 1、第 2 の暗号化情報とともに

に、記録される第 2 の暗号化情報の解読に有効な第 2 の暗号化キーが何であることを示す暗号化キー識別情報を記録することを特徴とするデジタル情報記録再生装置。

【請求項 5】 請求項 1 ないし請求項 4 のいずれかに記載のデジタル情報記録再生装置において、

前記第 1 の暗号化読取部、第 2 の暗号化読取部、第 1 の記憶手段、及び第 2 の記憶手段が、デジタル情報記録再生装置本体に対し着脱自在の電子回路ユニットに搭載されていることを特徴とするデジタル情報記録再生装置。

【請求項 6】 放送局より伝送される、情報を第 1 の期間ごとに变化する第 1 の暗号化キーを用いて暗号化した第 1 の暗号化情報、前記第 1 の暗号化キーと前記情報の属性情報を第 2 の期間ごとに变化する第 2 の暗号化キーにより暗号化した第 2 の暗号化情報、及び次の第 2 の期間に有効な第 2 の暗号化キーと個別の契約情報を第 3 の暗号化キーにより暗号化した第 3 の暗号化情報を受信する手段と、

受信した第 3 の暗号化情報を前記第 3 の暗号化キーを用いて暗号を解除して前記第 2 の暗号化キーと前記個別の契約情報を出力する第 1 の暗号化読取部と、

該第 1 の暗号化読取部が出力する第 2 の暗号化キーを次の第 2 の期間の間保持する記憶手段と、

受信した第 2 の暗号化情報を、一つ前の第 2 の期間に得られ前記第 1 の記憶手段に保持された第 2 の暗号化キーを用いて暗号を解除して前記第 1 の暗号化キーと前記情報の属性情報を出力する第 2 の暗号化読取部と、

受信した第 1 の暗号化情報を、前記第 2 の暗号化読取部より出力され、前記第 1 の暗号化読取部より出力された個別の契約情報と前記第 2 の暗号化読取部より出力された情報の属性情報との比較に基づいて与えられる、第 1 の暗号化キーを用いて暗号を解除して前記情報を得る第 3 の暗号化読取部と、

受信した第 3 の暗号化情報を次の第 2 の期間の間保持する暗号化情報保持手段と、

受信した第 1、及び第 2 の暗号化情報と前記暗号化情報保持手段に保持された一つ前の第 2 の期間に受信した第 3 の暗号化情報を記録、再生する記録再生手段とを備えたことを特徴とするデジタル情報記録再生装置。

【請求項 7】 請求項 6 記載のデジタル情報記録再生装置において、

上記第 3 の暗号化読取部は、再生時の直前に取得した個別の契約情報と前記第 2 の暗号化読取部より出力された情報の属性情報との比較に基づいて与えられる、第 1 の暗号化キーを用いて、上記記録再生手段が再生する第 1 の暗号化情報の暗号を解除するものであることを特徴とするデジタル情報記録再生装置。

【請求項 8】 請求項 6 記載のデジタル情報記録再生装置において、

記録時の個別の契約情報を保持する契約情報保持手段を

10

20

30

40

50

さらに備え、

上記第3の暗号化解読部は、上記契約情報保持手段が保持する記録時の個別の契約情報と前記第2の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて、上記記録再生手段が再生する第1の暗号化情報の暗号を解除するものであることを特徴とするデジタル情報記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、放送局から暗号化されて伝送されるデジタル情報を記録再生するデジタル情報記録再生装置に関するものである。

【0002】

【従来の技術】図7は、デジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成

(放送側)及び従来のデジタル情報記録再生装置(受信側)の構成を示す図であり、図において、1は映像情報、音声情報、及びデータを含むデジタル番組情報を第1の暗号化キー(Ks)を用いて暗号化して第1の暗号化情報を出力する第1の暗号化処理部、2は第1の暗号化キー(Ks)と上記番組情報の番組の属性情報を第2の暗号化キー(Kw)を用いて暗号化して第2の暗号化情報(ECM情報)を出力する第2の暗号化処理部、3は第2の暗号化キー(Kw)と受信者の個別の契約情報を第3の暗号化キーを用いて暗号化して第3の暗号化情報(EMM情報)を出力する第3の暗号化処理部である。

【0003】ここで、第1の暗号化キー(Ks)は第1の期間(数秒)ごとに異なる暗号化キーに切り替わるものであり、第2の暗号化キー(Kw)は第2の期間(1ヶ月～1年)ごとに異なる暗号化キーに切り替わるものである。また、第3の暗号化キーは受信の契約等をした時点で契約者に対して与えられるものであり、通常は切り替わることはないものである。

【0004】また、4は受信した第3の暗号化情報(EMM情報)をあらかじめ与えられた第3の暗号化キーを用いて解読し、第2の暗号化キーと契約情報を得る第1の暗号化解読部、7は第1の暗号化解読部4が出力する第2の暗号化キーを記憶し、一つ前の第2の期間に記憶した第2の暗号化キーを出力する記憶手段である。5は受信した第2の暗号化情報(ECM情報)を記憶手段7が出力する一つ前の第2の期間に受信した第2の暗号化キーを用いて解読し、第1の暗号化キーと番組の属性情報を得る第2の暗号化解読部、6は受信した第1の暗号化情報を第1の暗号化キーを用いて解読し、情報(映像、音声、データ)を得る第3の暗号化解読部である。8は第2の暗号化解読部5で得られた番組の属性情報と第1の暗号化解読部4で得られた契約情報とを比較して契約者が当該番組を視聴する資格を有するか否かの判定を行なう資格判定部であり、資格の有無に応じた制御信

号を出力し、第1の暗号化キー(Ks)を第3の暗号化解読部6に与えるか否かのスイッチングを行なう。

【0005】図8は記憶手段7の構成を示す図である。図に示すように、記憶手段7は、第1の暗号化解読部4が出力する第2の暗号化キーを受け取ってこれを保持する第1の記憶領域7aと、一つ前の第2の期間に受け取った第2の暗号化キーを保持しこれを第2の暗号化解読部5に対し出力する第2の記憶領域7bとを備えている。第1の記憶領域7aに保持された第2の暗号化キーは第2の期間が切り替わったとき、すなわち、第1の暗号化解読部4から受け取る第2の暗号化キーが変化するタイミングで第2の記憶領域7bに移され、それ以前に第2の記憶領域7bに保持されていた第2の暗号化キーは消去される。第1の記憶領域7aと第2の記憶領域7bとの間でこのような保持情報の受け渡しの動作が行なわれることにより、記憶手段7からは、常に、一つ前の第2の期間に取得した第2の暗号化キーが第2の暗号化解読部5に対して出力されるものである。

【0006】映像情報、音声情報、及びデータを含むデジタル番組情報は第1の暗号化処理部1において第1の暗号化キー(Ks)を用いて暗号化され、第1の暗号化情報として伝送される。第1の暗号化キー(Ks)は第1の期間(数秒)ごとに異なる暗号化キーに切り替わるものであり、受信側で第1の暗号化情報の解読を可能とするために、この順次切り替わる第1の暗号化キー(Ks)は番組の属性情報とともに第2の暗号化処理部2において第2の暗号化キー(Kw)を用いて暗号化され、第2の暗号化情報(ECM情報)として伝送される。第2の暗号化キー(Kw)は受信者の個別の契約情報とともに第3の暗号化処理部3において第3の暗号化キーを用いて暗号化され、第3の暗号化情報(EMM情報)として伝送される。第2の暗号化キー(Kw)は第2の期間(1ヶ月～1年)ごとに異なる暗号化キーに切り替わるものであり、ある第2の期間に伝送される第2の暗号化情報(ECM情報)を解読するための第2の暗号化キーは、その第2の期間の一つ前の第2の期間に第3の暗号化情報に含まれて伝送される。

【0007】デジタル情報記録再生装置側(受信側)では、第1の暗号化解読部4が、あらかじめ与えられている第3の暗号化キーを用いて第3の暗号化情報(EMM情報)の暗号化を解読し、第2の暗号化キー、及び個別契約情報を得る。取得された第2の暗号化キーは記憶手段7の第1の記憶領域7aに保持され、個別契約情報は資格判定部8に入力される。一方、第2の暗号化解読部5は、記憶手段7の第2の記憶領域7bに保持された一つ前の第2の期間に受信した第2の暗号化キーを用いて第2の暗号化情報(ECM情報)を解読し、第1の暗号化キー(Ks)、及び番組の属性情報を得る。資格判定部8は、第1の暗号化解読部4から得た個別の契約情報と第2の暗号化解読部5から得た番組の属性情報とを

比較して、契約者が当該番組を視聴する資格を有するか否かの判定をし、判定結果に応じた制御信号を出力する。スイッチSWは資格判定部8からの制御信号に応じて、第2の暗号化解読部で得られた第1の暗号化キー

(Ks)を第3の暗号化解読部6に対して提供、非提供のスイッチングを行なう。また、第3の暗号化解読部6は、第2の暗号化解読部で得られスイッチSWを介して提供される第1の暗号化キー(Ks)を用いて第1の暗号化情報を解読し、番組の情報(映像、音声、データ)を得る。

【0008】図9は、第2の期間と第1暗号化キー(Ks)、第2の暗号化キー(Kw)との関係を示すタイミングチャート図である。図において、上述もしたように、放送局側から第2の暗号化情報(ECM情報)に含まれて送信される第1の暗号化キーは、第2の期間の切り替わりとは無関係に第1の期間(数秒)毎に切り替わる。一方、第3の暗号化情報(EMM情報)に含まれて放送局側から送信される第2の暗号化キー、及び第2の暗号化情報(ECM情報)の解読に有効な第2の暗号化キーは第2の期間毎に切り替わる。図9において、T1の期間に第2の暗号化情報(ECM情報)の解読に有効な第2の暗号化キーはKw1であり、T2の期間に第2の暗号化情報(ECM情報)の解読に有効な第2の暗号化キーはKw2であり、T3の期間に第2の暗号化情報(ECM情報)の解読に有効な第2の暗号化キーはKw3である。また、T1の期間に放送局側から送信される第3の暗号化情報(EMM情報)に含まれて放送局側から送信される第2の暗号化キーはKw2であり、T2の期間に放送局側から送信される第3の暗号化情報(EMM情報)に含まれて放送局側から送信される第2の暗号化キーはKw4である。このように、ある第2の期間に放送局側から送信される第2の暗号化情報(ECM情報)の解読に有効な第2の暗号化キーは、一つ前の第2の期間に放送局側から送信される第3の暗号化情報(EMM情報)に含まれて放送局側から送信される第2の暗号化キーである。

【0009】次に、従来のデジタル情報記録再生装置におけるデジタル情報の記録再生動作について説明する。

【0010】図示しない制御手段より情報記録の指示を受けて、記録再生手段9は、第1の暗号化情報、及び第2の暗号化情報(ECM情報)を記録媒体に記録する。再生時には、再生した第2の暗号化情報(ECM情報)を第2の暗号化解読部5に対して出力し、再生した第1の暗号化情報を第3の暗号化解読部6に対して出力する。この再生時に記憶手段7からは、この再生時が属する第2の期間の一つ前の第2の期間に第3の暗号化情報(EMM情報)に含まれて放送局側から送信された第2

の暗号化キーが出力される。例えば、図9において、T2の期間に再生を行なう場合は、記憶手段7から出力される第2の暗号化キーはKw2であり、T3の期間に再生を行なう場合は、記憶手段7から出力される第2の暗号化キーはKw3である。一方、図9において、T2の期間に記録された第2の暗号化信号(ECM情報)の解読に有効な第2の暗号化キーはKw2であるので、このT2の期間に記録された第2の暗号化信号(ECM情報)は、T2の期間に再生を行なう場合にのみその解読が可能であり、T3以降の期間に再生を行なった場合にはその解読を行なうことはできない。すなわち、T2の期間に記録されたデジタル情報は、T2の期間にのみその再生を行なうことができるものである。

【0011】

【発明が解決しようとする課題】従来の暗号化されたデジタル情報を記録再生するデジタル情報記録再生装置は、上述のような構成となっているため、例えば、図9において、Aの時点で記録再生手段8に記録されたデジタル情報は(p1+p2)の期間再生が可能であるのに対し、Bの時点で記録再生手段8に記録されたデジタル情報はp2の期間しか再生することができず、さらに、第2の期間の切り替わりの直前に記録再生手段8に記録されたデジタル情報は記録後すぐに第2の期間が切り替わることにより、記憶手段7から出力される第2の暗号化キーが、記録された第2の暗号化情報(ECM情報)を解読するのに必要な第2の暗号化キーから、異なる第2の暗号化キーに切り替わってしまうため、記録した情報を再生することができない。

【0012】また、上述の不都合を回避するために、デジタル情報の記録時に、記録する第2の暗号化情報(ECM情報)を解読するのに必要な第2の暗号化キーを記録再生手段にいっしょに記録しておき、再生時に、記録された第2の暗号化情報(ECM情報)をこの記録再生手段に記録された第2の暗号化キーを用いて解読することが考えられるが、暗号解除情報を記録再生手段に記録しておくので、暗号を解読される危険性があり、デジタル情報の暗号化伝送システムにおけるセキュリティが低下するという問題がある。

【0013】この発明は、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を提供することを目的とする。

【0014】

【課題を解決するための手段】上記の課題を解決するために、本発明(請求項1)に係るデジタル情報記録再生装置は、放送局より伝送される、情報を第1の期間ごとに変化する第1の暗号化キーを用いて暗号化した第1の暗号化情報、前記第1の暗号化キーと前記情報の属性情報を第2の期間ごとに変化する第2の暗号化キーによ

り暗号化した第2の暗号化情報、及び次の第2の期間に有効な第2の暗号化キーと個別の契約情報を第3の暗号化キーにより暗号化した第3の暗号化情報を受信する手段と、受信した第3の暗号化情報を前記第3の暗号化キーを用いて暗号を解除して前記第2の暗号化キーと前記個別の契約情報を出力する第1の暗号化解除部と、該第1の暗号化解除部が出力する第2の暗号化キーを次の第2の期間の間保持する第1の記憶手段と、受信した第2の暗号化情報を、一つ前の第2の期間に得られ前記第1の記憶手段に保持された第2の暗号化キーを用いて暗号を解除して前記第1の暗号化キーと前記情報の属性情報を出力する第2の暗号化解除部と、受信した第1の暗号化情報を、前記第2の暗号化解除部より出力され、前記第1の暗号化解除部より出力された個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて暗号を解除して前記情報を得る第3の暗号化解除部と、受信した第1、及び第2の暗号化情報を記録、再生する記録再生手段と、前記第1の記憶手段に保持している第2の暗号化キーを前記第1の記憶手段のデータ変更後一定期間保持する第2の記憶手段とを備え、前記記録再生手段に記録された情報の再生時に、前記第2の暗号化解除部が、前記記録再生手段が再生した第2の暗号化情報を、前記第1または第2の記憶手段に保持された第2の暗号化キーを用いて暗号を解除するようにしたものである。

【0015】また、本発明（請求項2）に係るデジタル情報記録再生装置は、請求項1記載のデジタル情報記録再生装置において、前記記録再生手段が、第1、第2の暗号化情報とともに記録時の時間情報を記録するものである。

【0016】また、本発明（請求項3）に係るデジタル情報記録再生装置は、請求項2記載のデジタル情報記録再生装置において、前記記録再生手段に記録された第1、第2の暗号化情報を、該第1、第2の暗号化情報が前記記録再生手段に記録された時から上記第2の記憶手段が第2の暗号化キーを保持する上記一定期間を上限とする所定期間に限り再生可能とする制御手段をさらに備えたものである。

【0017】また、本発明（請求項4）に係るデジタル情報記録再生装置は、請求項1または請求項3記載のデジタル情報記録再生装置において、前記記録再生手段が、第1、第2の暗号化情報とともに、記録される第2の暗号化情報の解読に有効な第2の暗号化キーが何であるかを示す暗号化キー識別情報を記録するものである。

【0018】また、本発明（請求項5）に係るデジタル情報記録再生装置は、請求項1ないし請求項4のいずれかに記載のデジタル情報記録再生装置において、前記第1の暗号化解除部、第2の暗号化解除部、第1の記

憶手段、及び第2の記憶手段を、デジタル情報記録再生装置本体に対し着脱自在の電子回路ユニットに搭載したものである。

【0019】また、本発明（請求項6）に係るデジタル情報記録再生装置は、放送局より伝送される、情報を第1の期間ごとに变化する第1の暗号化キーを用いて暗号化した第1の暗号化情報、前記第1の暗号化キーと前記情報の属性情報を第2の期間ごとに变化する第2の暗号化キーにより暗号化した第2の暗号化情報、及び次の第2の期間に有効な第2の暗号化キーと個別の契約情報を第3の暗号化キーにより暗号化した第3の暗号化情報を受信する手段と、受信した第3の暗号化情報を前記第3の暗号化キーを用いて暗号を解除して前記第2の暗号化キーと前記個別の契約情報を出力する第1の暗号化解除部と、該第1の暗号化解除部が出力する第2の暗号化キーを次の第2の期間の間保持する記憶手段と、受信した第2の暗号化情報を、一つ前の第2の期間に得られ前記第1の記憶手段に保持された第2の暗号化キーを用いて暗号を解除して前記第1の暗号化キーと前記情報の属性情報を出力する第2の暗号化解除部と、受信した第1の暗号化情報を、前記第2の暗号化解除部より出力され、前記第1の暗号化解除部より出力された個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて暗号を解除して前記情報を得る第3の暗号化解除部と、受信した第3の暗号化情報を次の第2の期間の間保持する暗号化情報保持手段と、受信した第1、及び第2の暗号化情報と前記暗号化情報保持手段に保持された一つ前の第2の期間に受信した第3の暗号化情報を記録、再生する記録再生手段とを備えたものである。

【0020】また、本発明（請求項7）に係るデジタル情報記録再生装置は、請求項6記載のデジタル情報記録再生装置において、上記第3の暗号化解除部が、再生時の直前に取得した個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて、上記記録再生手段が再生する第1の暗号化情報の暗号を解除するものである。

【0021】また、本発明（請求項8）に係るデジタル情報記録再生装置は、請求項6記載のデジタル情報記録再生装置において、記録時の個別の契約情報を保持する契約情報保持手段をさらに備え、上記第3の暗号化解除部が、上記契約情報保持手段に保持された個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて、上記記録再生手段が再生する第1の暗号化情報の暗号を解除するものである。

【0022】

【発明の実施の形態】

実施の形態1. 以下、本発明の実施の形態1について、

図面を用いて説明する。図1はデジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態1によるデジタル情報記録再生装置の構成を示す図であり、図において図7と同一符号は同一または相当部分である。本実施の形態によるデジタル情報記録再生装置において、第1の記憶手段である記憶手段7は、図7に示す従来例の記憶手段7と同様、図8に示すような、第1の暗号化解読部4が出力する第2の暗号化キーを受け取ってこれを保持する第1の記憶領域7aと、一つ前の第2の期間に受け取った第2の暗号化キーを保持しこれを第2の暗号化解読部5に対し出力する第2の記憶領域7bとを備えている。また、10は第2の期間が切り替わるタイミングで記憶手段7の第2の記憶領域7bに保持されている第2の暗号化キーを受け取り、これを一定期間保持する第2の記憶手段である。

【0023】次に本実施の形態1によるデジタル情報記録再生装置の動作について説明する。映像情報、音声情報、及びデータを含むデジタル番組情報は第1の暗号化処理部1において第1の暗号化キー（Ks）を用いて暗号化され、第1の暗号化情報として伝送され、第1の暗号化キー（Ks）は番組の属性情報とともに第2の暗号化処理部2において第2の暗号化キー（Kw）を用いて暗号化され、第2の暗号化情報（ECM情報）として伝送され、第2の暗号化キー（Kw）は受信者の個別の契約情報とともに第3の暗号化処理部3において第3の暗号化キーを用いて暗号化され、第3の暗号化情報（EMM情報）として伝送される。

【0024】デジタル情報記録再生装置側（受信側）では、第1の暗号化解読部4が、あらかじめ与えられている第3の暗号化キーを用いて第3の暗号化情報（EMM情報）の暗号化を解読し、第2の暗号化キー、及び個別契約情報を得る。取得された第2の暗号化キーは記憶手段7の第1の記憶領域7aに保持され、個別契約情報は資格判定部8に入力される。記憶装置7の第1の記憶領域7aに保持された第2の暗号化キーは第2の期間が切り替わったとき、すなわち、第1の暗号化解読部4から受け取る第2の暗号化キーが変化するタイミングで第2の記憶領域7bに移され、それ以前に第2の記憶領域7bに保持されていた第2の暗号化キーは第2の記憶手段10に移され、ここで一定期間保持される。第1の記憶領域7aと第2の記憶領域7bとの間で上述のような保持情報の受け渡しの動作が行なわれることにより、記憶手段7からは、常に、一つ前の第2の期間に取得した第2の暗号化キーが第2の暗号化解読部5に対して出力される。第2の暗号化解読部5は、記憶手段7の第2の記憶領域7bに保持された一つ前の第2の期間に受信した第2の暗号化キーを用いて第2の暗号化情報（ECM情報）を解読し、第1の暗号化キー（Ks）、及び番組の属性情報を得る。資格判定部8は、第1の暗号化解読

部4から得た個別の契約情報と第2の暗号化解読部5から得た番組の属性情報とを比較して、契約者が当該番組を視聴する資格を有するか否かの判定をし、判定結果に応じた制御信号を出力する。スイッチSWは資格判定部8からの制御信号に応じて、第2の暗号化解読部で得られた第1の暗号化キー（Ks）を第3の暗号化解読部6に対して提供、非提供のスイッチングを行なう。また、第3の暗号化解読部6は、第2の暗号化解読部で得られスイッチSWを介して提供される第1の暗号化キー（Ks）を用いて第1の暗号化情報を解読し、番組の情報（映像、音声、データ）を得る。

【0025】図2は、本実施の形態1によるデジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。図において、上述もしたように、放送局側から第2の暗号化情報（ECM情報）に含まれて送信される第1の暗号化キーは、第2の期間の切り替わりとは無関係に第1の期間（数秒）毎に切り替わる。一方、第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キー、及び第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーは第2の期間毎に切り替わる。図2において、T1の期間に第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーはKw1であり、T2の期間に第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーはKw2であり、T3の期間に第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーはKw3である。また、T1の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーはKw2であり、T2の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーはKw3であり、T3の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーはKw4である。このように、ある第2の期間に放送局側から送信される第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーは、一つ前の第2の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーである。そして、記憶手段7が第2の暗号化解読手段5に対し出力する第2の暗号化キーは、T1の期間はKw1であり、T2の期間はKw2であり、T3の期間はKw3である。本実施の形態1によるデジタル情報記録再生装置では、さらに、第2の記憶手段10が、記憶手段7が出力する第2の暗号化キーが切り替わった後の一定期間、それまで記憶手段7が出力していた第2の暗号化キーを第2の暗号化解読手段5に対し出力する。

【0026】次に、本実施の形態1によるデジタル情報記録再生装置におけるデジタル情報の記録再生動作について説明する。図示しない記録再生手段制御手段よ

り情報記録の指示を受けて、記録再生手段 9 は、第 1 の暗号化情報、及び第 2 の暗号化情報（ECM 情報）を記録媒体に記録する。再生時には、再生した第 2 の暗号化情報（ECM 情報）を第 2 の暗号化読取部 5 に対して出力し、再生した第 1 の暗号化情報を第 3 の暗号化読取部 6 に対して出力する。この再生時に、図示しない記憶手段制御手段は、再生しようとしている情報の第 2 の暗号化情報が、記憶手段 7 が出力する第 2 の暗号化キー、あるいは第 2 の記憶手段 1 0 が出力する第 2 の暗号化キーのいずれかによって読取することができるかを判断し、読取可能と判断した場合は、記憶手段 7 または第 2 の記憶手段 1 0 が出力する、再生しようとしている情報の第 2 の暗号化情報の読取に有効な第 2 の暗号化キーが第 2 の暗号化読取部 5 に与えられるように制御する。

【0027】上記記憶手段制御手段の制御動作の具体例を説明する。この具体例においては、記録再生手段 9 にデジタル情報を記録する際に、記録される情報の第 2 の暗号化情報の読取に有効な第 2 の暗号化キーが何であることを示す暗号化キー識別情報を同時に記録しておく。この暗号化キー識別情報の記録は、たとえば放送局側で暗号化情報に付加して伝送する番組情報にこの暗号化キー識別情報を含めて伝送するようにすれば、この番組情報を暗号化情報とともに記録することにより、容易に達成できるものである。記録再生手段 9 が図示しない記録再生手段制御手段より情報再生の指示を受けると、記憶手段制御手段は、再生しようとしている情報の第 2 の暗号化情報の読取に有効な第 2 の暗号化キーが何であることを上記暗号化キー識別情報で認識し、記憶手段 7 の第 2 の記憶領域 7 b に保持された第 2 の暗号化キーおよび第 2 の記憶手段 1 0 に保持された第 2 の暗号化キーのいずれかが上記暗号化キー識別情報の示す第 2 の暗号化キーであるか否かを判断する。記憶手段 7 の第 2 の記憶領域 7 b に保持された第 2 の暗号化キーおよび第 2 の記憶手段 1 0 に保持された第 2 の暗号化キーのいずれもが、暗号化キー識別情報の示す第 2 の暗号化キーでない場合は、図示しない表示手段に、暗号が読取できないことを表示する。記憶手段 7 の第 2 の記憶領域 7 b に保持された第 2 の暗号化キーおよび第 2 の記憶手段 1 0 に保持された第 2 の暗号化キーのいずれかが暗号化キー識別情報の示す第 2 の暗号化キーである場合は、暗号化キー識別情報の示す第 2 の暗号化キーである方の第 2 の暗号化キーが第 2 の暗号化読取手段 5 に対して出力されるように記憶手段 7 および第 2 の記憶手段 1 0 を制御する。

【0028】例えば、図 2 において、「REC」で示すタイミングでデジタル情報を記録した場合、記録媒体には、第 1 の暗号化情報、及び第 2 の暗号化情報（ECM 情報）とともに、記録される第 2 の暗号化情報の読取に有効な第 2 の暗号化キーが Kw 2 であることを示す暗号化キー識別情報が同時に記録される。記録したデジタル情報の再生時が図 2 中の P 1 の期間であるときは、

記憶手段 7 の第 2 の記憶領域 7 b に保持された第 2 の暗号化キーが Kw 2 であるので、記憶手段制御手段は記憶手段 7 が第 2 の暗号化読取手段 5 に対して第 2 の暗号化キーを出力するように制御する。また、記録したデジタル情報の再生時が図 2 中の P 2 の期間であるときは、第 2 の記憶手段 1 0 に保持された第 2 の暗号化キーが Kw 2 であるので、記憶手段制御手段は第 2 の記憶手段 1 0 が第 2 の暗号化読取手段 5 に対して第 2 の暗号化キーを出力するように制御する。

10 【0029】このような、本実施の形態 1 によるデジタル情報記録再生装置では、第 2 の期間が切り替わる直前にデジタル情報を記録した場合でも、第 2 の記憶手段に第 2 の暗号化キーが保持されている一定期間は、記録したデジタル情報の再生を可能とできる。しかも、記録再生手段には、従来のデジタル情報記録再生装置と同様、第 1、第 2 の暗号化情報を記録するものであるため、記録再生手段に暗号化キーそのものを記録する場合のような、デジタル情報の暗号化伝送システムにおけるセキュリティの低下を招くことはない。

20 【0030】このように、本実施の形態 1 によるデジタル情報記録再生装置では、第 1 の記憶手段である記憶手段 7 に保持している第 2 の暗号化キーを記憶手段 7 のデータ変更後一定期間保持する第 2 の記憶手段 1 0 とを備え、第 1、第 2 の暗号化情報を記録、再生する記録再生手段 9 が、記録した第 1、第 2 の暗号化情報を再生するときに、第 2 の暗号化情報（ECM 情報）を読取する第 2 の暗号化読取部が、前記録再生手段が再生した第 2 の暗号化情報を、前記第 1 または第 2 の記憶手段に保持された第 2 の暗号化キーを用いて暗号を解除する構成としたから、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を実現できる。

30 【0031】なお、上記説明では、記録再生手段 9 にデジタル情報を記録する際に、記録される情報の第 2 の暗号化情報の読取に有効な第 2 の暗号化キーが何であることを示す暗号化キー識別情報を同時に記録し、記憶手段制御手段が、この暗号化キー識別情報と記憶手段 7 の第 2 の記憶領域 7 b に保持された第 2 の暗号化キーおよび第 2 の記憶手段 1 0 に保持された第 2 の暗号化キーとを比較して、暗号化キー識別情報の示す第 2 の暗号化キーである方の第 2 の暗号化キーが第 2 の暗号化読取手段 5 に対して出力されるように記憶手段 7 および第 2 の記憶手段 1 0 を制御する構成としたが、記録再生手段 9 にデジタル情報を記録する際に、その記録日時情報を同時に記録し、記憶手段制御手段が、再生時がこの記録日時情報が示す時が属する第 2 の期間と同じ第 2 の期間に属するときは記憶手段 7 に保持された第 2 の暗号化キーが第 2 の暗号化読取手段 5 に対して出力されるように、また、再生時がこの記録日時情報が示す時が属する第 2 の

期間の次の第2の期間であってかつ第2の記憶手段10が第2の暗号化キーを保持している一定期間に属するときは第2の記憶手段10に保持された第2の暗号化キーが第2の暗号化読取手段5に対して出力されるように記憶手段7および第2の記憶手段10を制御するようにしてもよい。

【0032】また、本実施の形態1において、第1の暗号化読取部4、第2の暗号化読取部5、記憶手段7、第2の記憶手段10を、ICカード等、デジタル情報記録再生装置本体に対し着脱自在な電子回路ユニットに搭載することにより、複数のデジタル情報記録再生装置のうちの一つのデジタル情報記録再生装置において取得した第2の暗号化キーを他のデジタル情報記録再生装置においても使用できるので、長時間の不使用のために当該他のデジタル情報記録再生装置が第2の暗号化キーを取得していない場合にも、情報の再生を行なうことができるデジタル情報記録再生装置を実現することができるものである。

【0033】実施の形態2。以下、本発明の実施の形態2について、図面を用いて説明する。図3はデジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態2によるデジタル情報記録再生装置の構成を示す図であり、図において図1と同一符号は同一または相当部分である。

【0034】上述のように、上記実施の形態1によるデジタル情報記録再生装置によれば、第2の期間が切り替わる直前にデジタル情報を記録した場合にも、少なくとも第2の記憶手段10に第2の暗号化キーが保持されている一定期間は、記録したデジタル情報を再生できる。しかしながら、この実施の形態1によるデジタル情報記録再生装置では、第2の期間のどの時点でデジタル情報を記録したかによって、再生できる期間の長さが異なる。

【0035】本実施の形態2によるデジタル情報記録再生装置は、実施の形態1によるデジタル情報記録再生装置において、記録再生手段9にデジタル情報を記録する際に、その記録日時情報を同時に記録し、図示しない情報再生制御手段により、前記記録再生手段に記録された第1、第2の暗号化情報を、該第1、第2の暗号化情報が記録再生手段9に記録された時から第2の記憶手段10が第2の暗号化キーを保持する一定期間を上限とする所定期間に限り再生可能とするように制御する構成としたものである。

【0036】以下、本実施の形態2によるデジタル情報記録再生装置の記録再生動作について説明する。図4は本実施の形態2によるデジタル情報記録再生装置の再生動作を説明するためのフローチャート図である。

【0037】図示しない記録再生手段制御手段より情報記録の指示を受けて、記録再生手段9は、第1の暗号化

情報、及び第2の暗号化情報（ECM情報）を記録媒体に記録する。このとき、記録時の日時情報、及び記録される第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーが何であることを示す暗号化キー識別情報を同時に記録する。この暗号化キー識別情報の記録は、たとえば放送局側で暗号化情報に付加して伝送する番組情報にこの暗号化キー識別情報を含めて伝送するようにすれば、この番組情報を暗号化情報とともに記録することにより、容易に達成できるものである。

- 10 【0038】記録再生手段9は図示しない記録再生手段制御手段より情報再生の指示を受けると、再生した第2の暗号化情報（ECM情報）を第2の暗号化読取部5に対して出力し、再生した第1の暗号化情報を第3の暗号化読取部6に対して出力する。以降の動作は図4に示すフローチャートに沿って説明する。図示しない再生制御手段は、第2の暗号化読取部5に入力される第2の暗号化情報（ECM情報）が、放送を受信した信号であるか、記録再生手段9からの再生信号であるかを検知し（ステップS1）、記録再生手段9からの再生信号であるときは、この第2の暗号化情報が記録された時を示す日時情報を再生信号より抽出し、この日時情報と現在日時を比較して、現在日時が記録時から所定の期間（再生可能期間）内であるか否かを判定する（ステップS2）。ここで再生可能期間は、第2の記憶手段10に第2の暗号化キーが保持される一定期間を上限とする所定の期間である。再生制御手段は、再生有効期限内でないと判断したときは図示しない表示手段に期限がすぎていることを表示し（ステップS3）、処理を終了し、再生有効期限内であると判断したときは、図示しない記憶手段制御手段に対し、次ステップの実行を行なう指示を出す。記憶手段制御手段は、再生信号より暗号化キー識別情報を抽出し（ステップS4）、再生しようとしている情報の第2の暗号化情報の解読に有効な第2の暗号化キーが何であることを認識し、記憶手段7の第2の記憶領域7bに保持された第2の暗号化キーおよび第2の記憶手段10に保持された第2の暗号化キーのいずれかが上記暗号化キー識別情報の示す第2の暗号化キーであるか否かを判断する（ステップS5）。記憶手段7の第2の記憶領域7bに保持された第2の暗号化キーおよび第2の記憶手段10に保持された第2の暗号化キーのいずれもが、暗号化キー識別情報の示す第2の暗号化キーでない場合は、図示しない表示手段に、暗号が解読できないことを表示し（ステップS6）、処理を終了する。記憶手段7の第2の記憶領域7bに保持された第2の暗号化キーおよび第2の記憶手段10に保持された第2の暗号化キーのいずれかが暗号化キー識別情報の示す第2の暗号化キーである場合は、暗号化キー識別情報の示す第2の暗号化キーである方の第2の暗号化キーが第2の暗号化読取手段5に対して出力されるように記憶手段7および第2の記憶手段10を制御する。第2の暗号化読取手段
- 20
- 30
- 40
- 50

5はこの第2の暗号化キーを用いて第2の暗号化情報（ECM情報）を解読し、第1の暗号化キーと番組の属性情報を出力する（ステップS7）。資格判定部8は第2の暗号化解読手段5が出力する番組の属性情報と個別の契約情報とを比較してユーザが当該番組の視聴資格を有するか否かを判定し（ステップS8）、番組のデコードが可能か否かを判断する（ステップS9）。デコード不可能と判断した場合は第1の暗号化キーが第3の暗号化解読部6に提供されないようにスイッチSWを制御するとともに、図示しない表示手段に、暗号が解読できないことを表示し（ステップS6）、処理を終了する。一方、デコード可能と判断した場合は第1の暗号化キーが第3の暗号化解読部6に提供されるようにスイッチSWを制御する。第3の暗号化解読部6は第2の暗号化解読手段5からスイッチSWを介して入力される第1の暗号化キーを用いて記録再生部9が再生する第1の暗号化情報の暗号を解読し（ステップS10）、番組の情報（映像、音声、データ）を得る。

【0039】このように、本実施の形態2によるデジタル情報記録再生装置では、第1の記憶手段である記憶手段7に保持している第2の暗号化キーを記憶手段7のデータ変更後一定期間保持する第2の記憶手段10を備え、第1、第2の暗号化情報を記録、再生する記録再生手段9が、記録した第1、第2の暗号化情報を再生するときに、第2の暗号化情報（ECM情報）を解読する第2の暗号化解読部が、前記録再生手段が再生した第2の暗号化情報を、前記第1または第2の記憶手段に保持された第2の暗号化キーを用いて暗号を解除する構成とするとともに、記録再生手段9にデジタル情報を記録する際に、その記録日時情報を同時に記録し、図示しない情報再生制御手段により、前記録再生手段に記録された第1、第2の暗号化情報を、該第1、第2の暗号化情報が記録再生手段9に記録された時から第2の記憶手段10が第2の暗号化キーを保持する一定期間を上限とする所定期間に限り再生可能とするように制御する構成としたから、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、第2の期間のどの時点でデジタル情報を記録した場合であっても、一律に一定期間、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を実現できる。

【0040】なお、上記説明では、記録再生手段9にデジタル情報を記録する際に、記録される情報の第2の暗号化情報の解読に有効な第2の暗号化キーが何であるかを示す暗号化キー識別情報を同時に記録し、記憶手段制御手段が、この暗号化キー識別情報と記憶手段7の第2の記憶領域7bに保持された第2の暗号化キーおよび第2の記憶手段10に保持された第2の暗号化キーとを比較して、暗号化キー識別情報の示す第2の暗号化キーである方の第2の暗号化キーが第2の暗号化解読手段5に対して出力されるように記憶手段7および第2の記憶

手段10を制御する構成としたが、記憶手段制御手段が、再生時が、記録日時情報が示す時が属する第2の期間と同じ第2の期間に属するときは記憶手段7に保持された第2の暗号化キーが第2の暗号化解読手段5に対して出力されるように、また、再生時が、記録日時情報が示す時が属する第2の期間の次の第2の期間に属するときは第2の記憶手段10に保持された第2の暗号化キーが第2の暗号化解読手段5に対して出力されるように記憶手段7および第2の記憶手段10を制御するようにしてもよい。

【0041】また、本実施の形態2において、第1の暗号化解読部4、第2の暗号化解読部5、記憶手段7、第2の記憶手段10を、ICカード等、デジタル情報記録再生装置本体に対し着脱自在な電子回路ユニットに搭載することにより、複数のデジタル情報記録再生装置のうちの一つのデジタル情報記録再生装置において取得した第2の暗号化キーを他のデジタル情報記録再生装置においても使用できるので、長時間の不使用のために当該他のデジタル情報記録再生装置が第2の暗号化キーを取得していない場合にも、情報の再生を行なうことができるデジタル情報記録再生装置を実現することができるものである。

【0042】実施の形態3. 以下、本発明の実施の形態3について、図面を用いて説明する。図5はデジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態2によるデジタル情報記録再生装置の構成を示す図であり、図において図1と同一符号は同一または相当部分である。また、11は受信した第3の暗号化情報（EMM情報）を次の第2の期間の間保持するEMM情報保持手段である。

【0043】次に本実施の形態3によるデジタル情報記録再生装置の動作について説明する。本実施の形態3によるデジタル情報記録再生装置の通常のデジタル情報の受信、表示動作は、従来のデジタル情報記録再生装置と同様である。

【0044】すなわち、第1の暗号化解読部4が、あらかじめ与えられている第3の暗号化キーを用いて受信した第3の暗号化情報（EMM情報）の暗号化を解読し、第2の暗号化キー、及び個別契約情報を得る。取得された第2の暗号化キーは記憶手段7の第1の記憶領域7aに保持され、個別契約情報は資格判定部8に入力される。記憶装置7の第1の記憶領域7aに保持された第2の暗号化キーは第2の期間が切り替わったとき、すなわち、第1の暗号化解読部4から受け取る第2の暗号化キーが変化するタイミングで第2の記憶領域7bに移され、それ以前に第2の記憶領域7bに保持されていた第2の暗号化キーは消去される。第1の記憶領域7aと第2の記憶領域7bとの間で上述のような保持情報の受け渡しの動作が行なわれることにより、記憶手段7から

は、常に、一つ前の第2の期間に取得した第2の暗号化キーが第2の暗号化読部5に対して出力される。第2の暗号化読部5は、記憶手段7の第2の記憶領域7bに保持された一つ前の第2の期間に受信した第2の暗号化キーを用いて第2の暗号化情報（ECM情報）を解読し、第1の暗号化キー（Ks）、及び番組の属性情報を得る。資格判定部8は、第1の暗号化読部4から得た個別の契約情報と第2の暗号化読部5から得た番組の属性情報とを比較して、契約者が当該番組を視聴する資格を有するか否かの判定をし、判定結果に応じた制御信号を出力する。スイッチSWは資格判定部8からの制御信号に応じて、第2の暗号化読部で得られた第1の暗号化キー（Ks）を第3の暗号化読部6に対して提供、非提供のスイッチングを行なう。また、第3の暗号化読部6は、第2の暗号化読部で得られスイッチSWを介して提供される第1の暗号化キー（Ks）を用いて第1の暗号化情報を解読し、番組の情報（映像、音声、データ）を得る。

【0045】図6は、本実施の形態3によるデジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。図において、放送局側から第2の暗号化情報（ECM情報）に含まれて送信される第1の暗号化キーは、第2の期間の切り替わりとは無関係に第1の期間（数秒）毎に切り替わる。一方、第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キー、及び第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーは第2の期間毎に切り替わる。図2において、T1の期間に第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーはKw1であり、T2の期間に第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーはKw2であり、T3の期間に第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーはKw3である。また、T1の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーはKw2であり、T2の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーはKw3であり、T3の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーはKw4である。このように、ある第2の期間に放送局側から送信される第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーは、一つ前の第2の期間に放送局側から送信される第3の暗号化情報（EMM情報）に含まれて放送局側から送信される第2の暗号化キーである。

【0046】また、本実施の形態3によるデジタル情報記録再生装置では、受信した第3の暗号化情報（EMM情報）を、EMM情報保持手段11が、次の第2の期間の間保持する。すなわち、図5において、T1の期間

は、これに含まれる第2の暗号化キーがKw1であるEMM情報がEMM情報保持手段11に保持され、T2の期間、これに含まれる第2の暗号化キーがKw2であるEMM情報がEMM情報保持手段11に保持され、T3の期間は、これに含まれる第2の暗号化キーがKw3であるEMM情報がEMM情報保持手段11に保持される。

【0047】次に、本実施の形態3によるデジタル情報記録再生装置におけるデジタル情報の記録再生動作について説明する。図示しない記録再生手段制御手段より情報記録の指示を受けて、記録再生手段9は、受信した第1の暗号化情報、第2の暗号化情報（ECM情報）、及びEMM情報保持手段に11に保持された第3の暗号化情報（EMM情報）を記録媒体に記録する。すなわち、記録媒体には、受信した第1の暗号化情報、第2の暗号化情報（ECM情報）とともに、当該受信した第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーが暗号化されて含まれる第3の暗号化情報（EMM情報）が記録されることとなる。再生時に記録再生手段9は、再生した第3の暗号化情報（EMM情報）を第1の暗号化読部4に対して出力し、再生した第2の暗号化情報（ECM情報）を第2の暗号化読部5に対して出力し、再生した第1の暗号化情報を第3の暗号化読部6に対して出力する。第1の暗号化読部4は、通常の動作と同様に、第3の暗号化キーを用いて、記録再生手段9が再生した第3の暗号化情報（EMM情報）を解読し、第2の暗号化キーを出力する。なお、個別の契約情報については、受信した第3の暗号化情報（EMM情報）を解読して得られた契約情報のうち、再生時の直前に得られたものを用いる。ここで出力される第2の暗号化キーは記録再生手段9が再生する第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーである。第2の暗号化読部5は、記録情報の再生時には、記憶手段7が出力する第2の暗号化キーではなく、第1の暗号化読部4が出力する第2の暗号化キーを用いるように制御される。従って、第2の暗号化読部5は、第1の暗号化読部4が出力する、記録再生手段9が再生する第2の暗号化情報（ECM情報）の解読に有効な第2の暗号化キーを用いて、入力される第2の暗号化情報（ECM情報）の解読を行なうことができる。以降は通常の動作と同様に、第2の暗号化読部で得られスイッチSWを介して提供される第1の暗号化キー（Ks）を用いて第1の暗号化情報を解読し、番組の情報（映像、音声、データ）を得る。

【0048】このように、本実施の形態3によるデジタル情報記録再生装置では、受信し第3の暗号化情報（EMM情報）を次の第2の期間の間保持するEMM情報保持手段11を備え、記録再生手段9が、受信した第1、第2の暗号化情報とともに上記EMM情報保持手段に保持された第3の暗号化情報を記録する構成としたか

ら、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、記録したデジタル情報を確実に再生可能とできるデジタル情報記録再生装置を実現できる。

【0049】なお、上記実施の形態3では、個別の契約情報については、再生時の直前に取得したものを資格判定に用いる構成としたが、情報の記録時の個別の契約情報を保持する手段を設け、再生時にこの保持された契約情報を資格判定部8に入力する構成としてもよい。このような構成とすれば、再生時直前に取得した個別の契約情報が、記録された情報の視聴を不可とする内容となっている場合でも、記録された情報の再生を行なうことができ、個別の契約情報の変更によって、記録した情報が再生できないという不都合が生じることを回避できる。

【0050】

【発明の効果】以上のように、本発明（請求項1）に係るデジタル情報記録再生装置によれば、放送局より伝送される、情報を第1の期間ごとに变化する第1の暗号化キーを用いて暗号化した第1の暗号化情報、前記第1の暗号化キーと前記情報の属性情報を第2の期間ごとに变化する第2の暗号化キーにより暗号化した第2の暗号化情報、及び次の第2の期間に有効な第2の暗号化キーと個別の契約情報を第3の暗号化キーにより暗号化した第3の暗号化情報を受信する手段と、受信した第3の暗号化情報を前記第3の暗号化キーを用いて暗号を解除して前記第2の暗号化キーと前記個別の契約情報を出力する第1の暗号化解除部と、該第1の暗号化解除部が出力する第2の暗号化キーを次の第2の期間の間保持する第1の記憶手段と、受信した第2の暗号化情報を、一つ前の第2の期間に得られ前記第1の記憶手段に保持された第2の暗号化キーを用いて暗号を解除して前記第1の暗号化キーと前記情報の属性情報を出力する第2の暗号化解除部と、受信した第1の暗号化情報を、前記第2の暗号化解除部より出力され、前記第1の暗号化解除部より出力された個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて暗号を解除して前記情報を得る第3の暗号化解除部と、受信した第1、及び第2の暗号化情報を記録、再生する記録再生手段と、前記第1の記憶手段に保持している第2の暗号化キーを前記第1の記憶手段のデータ変更後一定期間保持する第2の記憶手段とを備え、前記記録再生手段に記録された情報の再生時に、前記第2の暗号化解除部が、前記記録再生手段が再生した第2の暗号化情報を、前記第1または第2の記憶手段に保持された第2の暗号化キーを用いて暗号を解除する構成としたから、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を実現できる効果がある。

【0051】また、本発明（請求項2）に係るデジタル情報記録再生装置によれば、請求項1記載のデジタル情報記録再生装置において、前記記録再生手段が、第1、第2の暗号化情報とともに記録時の時間情報を記録するものとしたから、再生時が属する第2の期間と記録時が属する第2の期間の比較に基づいて、前記第1または第2の記憶手段に保持された第2の暗号化キーのいずれかを用いて記録再生手段が再生した第2の暗号化情報の暗号を解除でき、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を実現できる効果がある。

【0052】また、本発明（請求項3）に係るデジタル情報記録再生装置によれば、請求項2記載のデジタル情報記録再生装置において、前記記録再生手段に記録された第1、第2の暗号化情報を、該第1、第2の暗号化情報が前記記録再生手段に記録された時から上記第2の記憶手段が第2の暗号化キーを保持する上記一定期間を上限とする所定期間内に限り再生可能とする制御手段をさらに備えた構成としたから、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、第2の期間のどの時点でデジタル情報を記録した場合であっても、一律に一定期間、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を実現できる効果がある。

【0053】また、本発明（請求項4）に係るデジタル情報記録再生装置によれば、請求項1または請求項3記載のデジタル情報記録再生装置において、前記記録再生手段が、第1、第2の暗号化情報とともに、記録される第2の暗号化情報の解読に有効な第2の暗号化キーが何であることを示す暗号化キー識別情報を記録するようにしたから、前記第1または第2の記憶手段に保持された第2の暗号化キーのうち暗号化キー識別情報が示す第2の暗号化キーを用いて記録再生手段が再生した第2の暗号化情報の暗号を解除でき、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、第2の期間のどの時点でデジタル情報を記録した場合であっても、一律に一定期間、記録したデジタル情報の再生を可能とできるデジタル情報記録再生装置を実現できる効果がある。

【0054】また、本発明（請求項5）に係るデジタル情報記録再生装置によれば、請求項1ないし請求項4のいずれかに記載のデジタル情報記録再生装置において、前記第1の暗号化解除部、第2の暗号化解除部、第1の記憶手段、及び第2の記憶手段を、デジタル情報記録再生装置本体に対し着脱自在の電子回路ユニットに搭載したから、請求項1ないし請求項4に係る発明のそれぞれによる効果に加えて、複数のデジタル情報記録再生装置のうちの一つのデジタル情報記録再生装置に

において取得した第2の暗号化キーを他のデジタル情報記録再生装置においても使用でき、長時間の不使用のために当該他のデジタル情報記録再生装置が第2の暗号化キーを取得していない場合にも、情報の再生を行なうことができるデジタル情報記録再生装置を実現することができる効果がある。

【0055】また、本発明（請求項6）に係るデジタル情報記録再生装置によれば、放送局より伝送される、情報を第1の期間ごとに变化する第1の暗号化キーを用いて暗号化した第1の暗号化情報、前記第1の暗号化キーと前記情報の属性情報を第2の期間ごとに变化する第2の暗号化キーにより暗号化した第2の暗号化情報、及び次の第2の期間に有効な第2の暗号化キーと個別の契約情報を第3の暗号化キーにより暗号化した第3の暗号化情報を受信する手段と、受信した第3の暗号化情報を前記第3の暗号化キーを用いて暗号を解除して前記第2の暗号化キーと前記個別の契約情報を出力する第1の暗号化解除部と、該第1の暗号化解除部が出力する第2の暗号化キーを次の第2の期間の間保持する記憶手段と、受信した第2の暗号化情報を、一つ前の第2の期間に得られ前記第1の記憶手段に保持された第2の暗号化キーを用いて暗号を解除して前記第1の暗号化キーと前記情報の属性情報を出力する第2の暗号化解除部と、受信した第1の暗号化情報を、前記第2の暗号化解除部より出力され、前記第1の暗号化解除部より出力された個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて暗号を解除して前記情報を得る第3の暗号化解除部と、受信した第3の暗号化情報を次の第2の期間の間保持する暗号化情報保持手段と、受信した第1、及び第2の暗号化情報と前記暗号化情報保持手段に保持された一つ前の第2の期間に受信した第3の暗号化情報を記録、再生する記録再生手段とを備えた構成としたから、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、記録したデジタル情報を確実に再生可能とできるデジタル情報記録再生装置を実現できる効果がある。

【0056】また、本発明（請求項7）に係るデジタル情報記録再生装置によれば、請求項6に記載のデジタル情報記録再生装置において、上記第3の暗号化解除部が、再生時の直前に取得した個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて、上記記録再生手段が再生する第1の暗号化情報の暗号を解除する構成としたから、デジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、記録したデジタル情報を、再生時の契約情報により再生可能な番組については、再生可能とできるデジタル情報記録再生装置を実現できる効果がある。

【0057】また、本発明（請求項8）に係るディジタ

ル情報記録再生装置によれば、請求項6記載のデジタル情報記録再生装置において、記録時の個別の契約情報を保持する契約情報保持手段をさらに備え、上記第3の暗号化解除部が、上記契約情報保持手段に保持された個別の契約情報と前記第2の暗号化解除部より出力された情報の属性情報との比較に基づいて与えられる、第1の暗号化キーを用いて、上記記録再生手段が再生する第1の暗号化情報の暗号を解除する構成としたから、再生時直前に取得した個別の契約情報が、記録された情報の視聴を不可とする内容となっている場合でも、記録された情報の再生を行なうことができ、個別の契約情報の変更によって、記録した情報が再生できないという不都合が生じることを回避できる効果がある。

【図面の簡単な説明】

【図1】 デジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態1によるデジタル情報記録再生装置の構成を示す図である。

【図2】 本発明の実施の形態1によるデジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。

【図3】 デジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態2によるデジタル情報記録再生装置の構成を示す図である。

【図4】 本発明の実施の形態2によるデジタル情報記録再生装置の再生動作を説明するためのフローチャート図である。

【図5】 デジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態3によるデジタル情報記録再生装置の構成を示す図である。

【図6】 本発明の実施の形態3によるデジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。

【図7】 デジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び従来のデジタル情報記録再生装置の構成を示す図である。

【図8】 記憶手段7の構成を示す図である。

【図9】 従来のデジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。

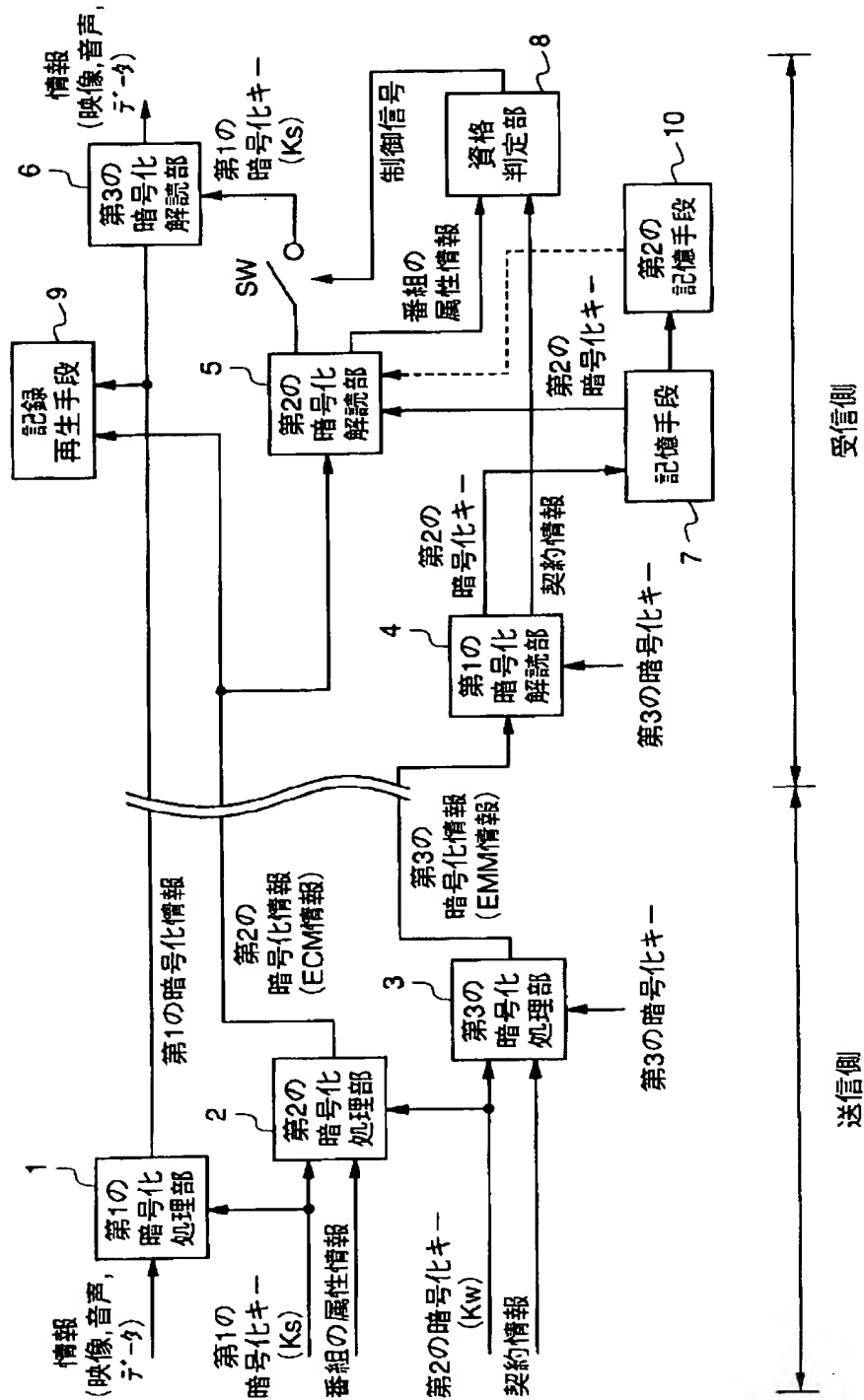
【符号の説明】

- 1 第1の暗号化処理部
- 2 第2の暗号化処理部
- 3 第3の暗号化処理部
- 4 第1の暗号化解除部
- 5 第2の暗号化解除部
- 6 第3の暗号化解除部
- 7 記憶手段

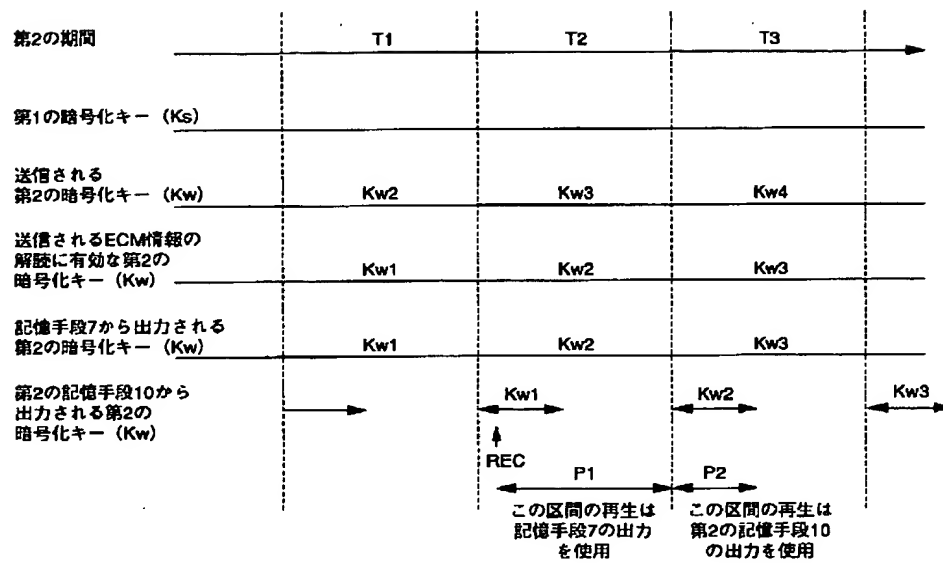
- 7 a 第1の記憶領域
7 b 第2の記憶領域
8 資格判定部

- * 9 記録再生手段
10 第2の記憶手段
* 11 EMM情報保持手段

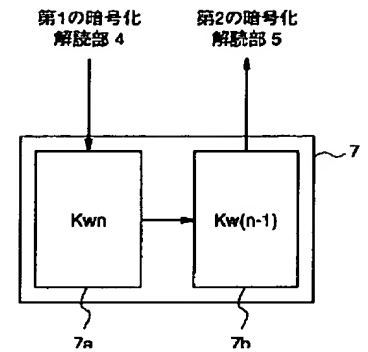
【図1】



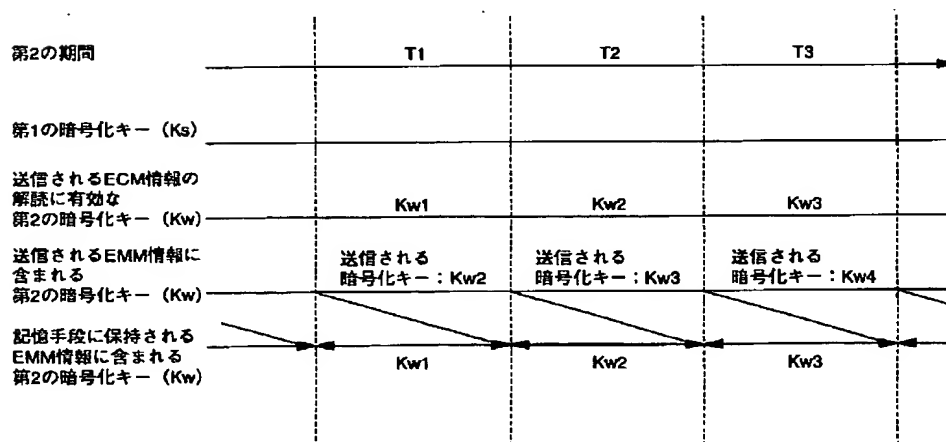
【図2】



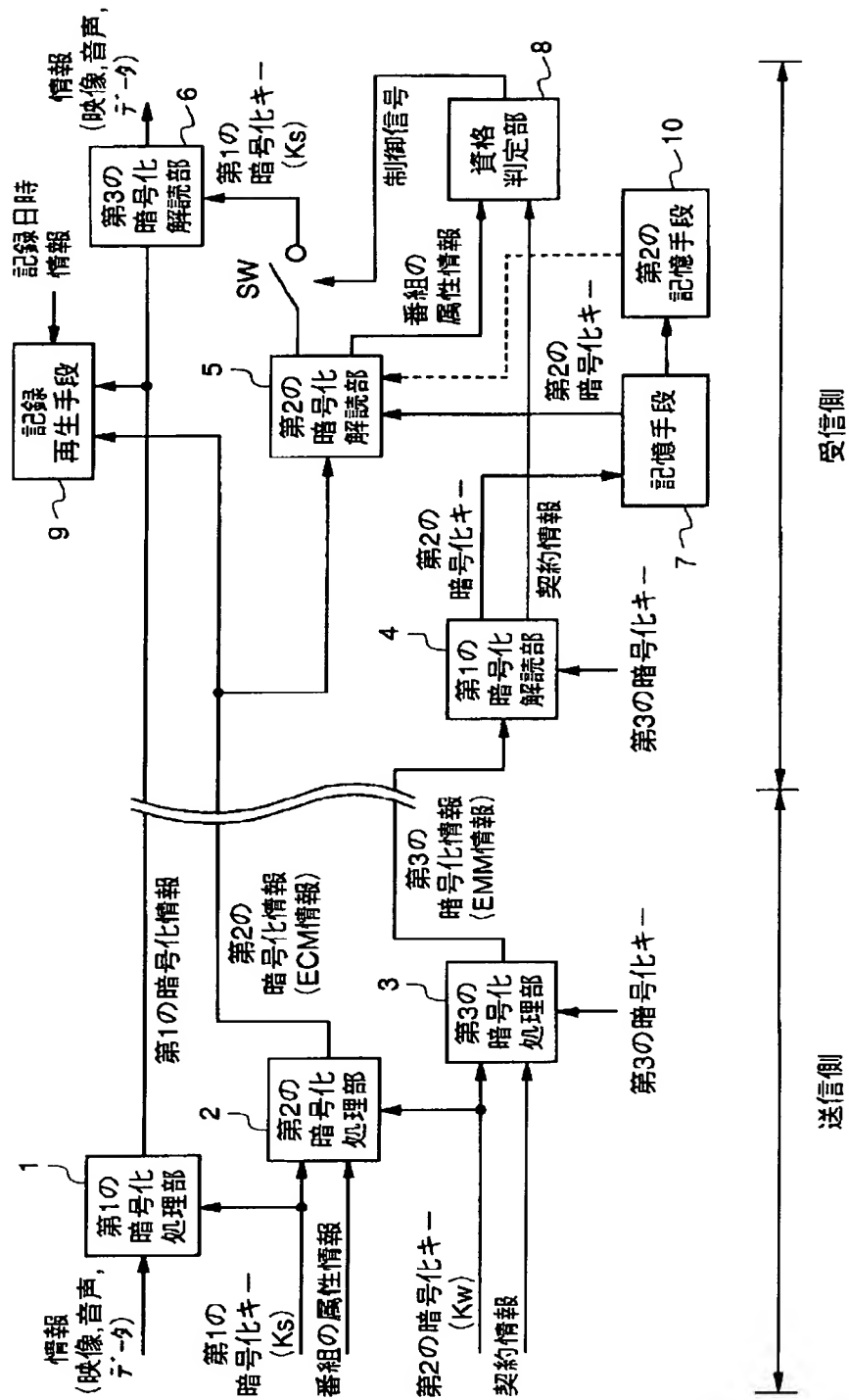
【図8】



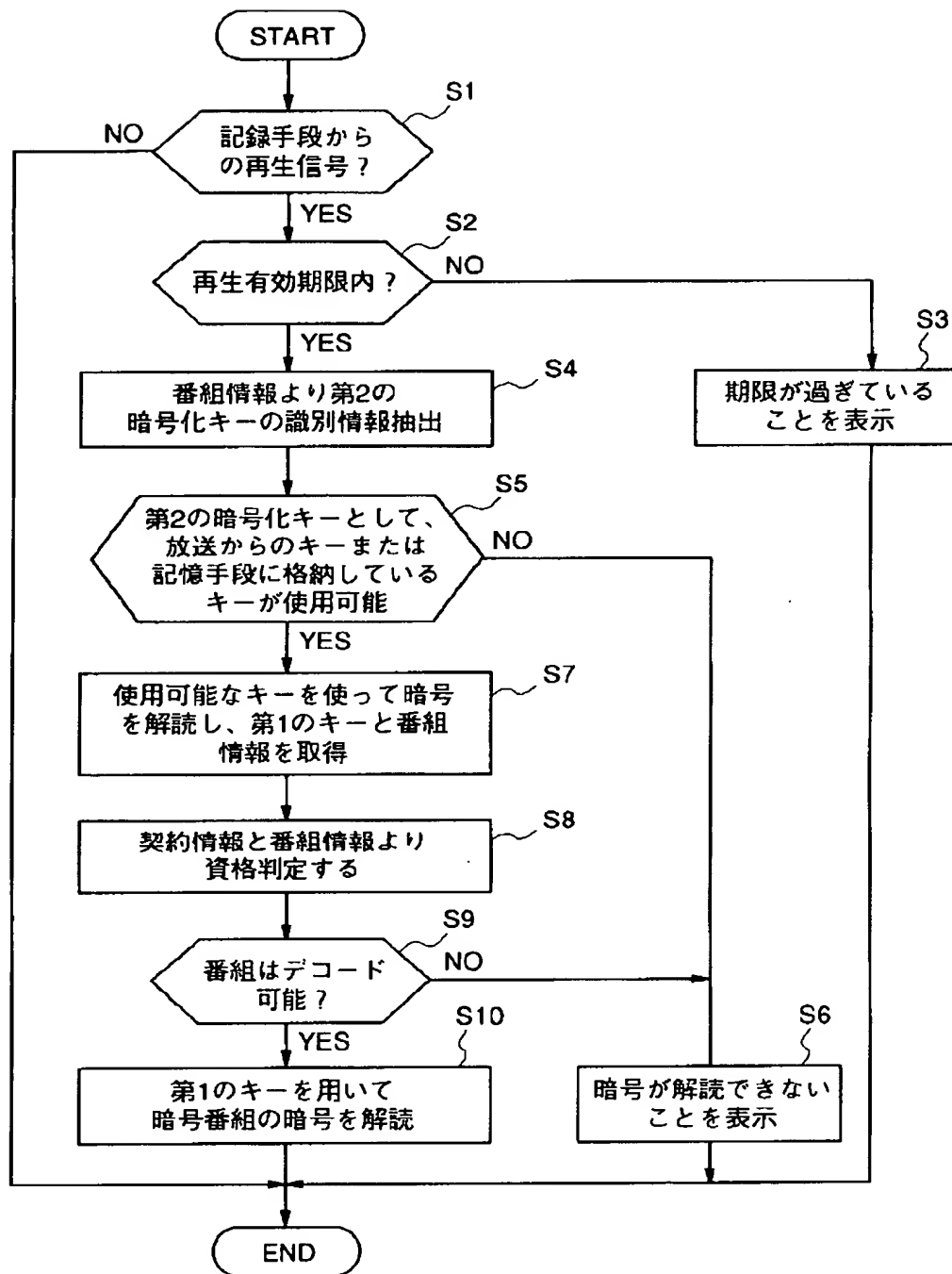
【図6】



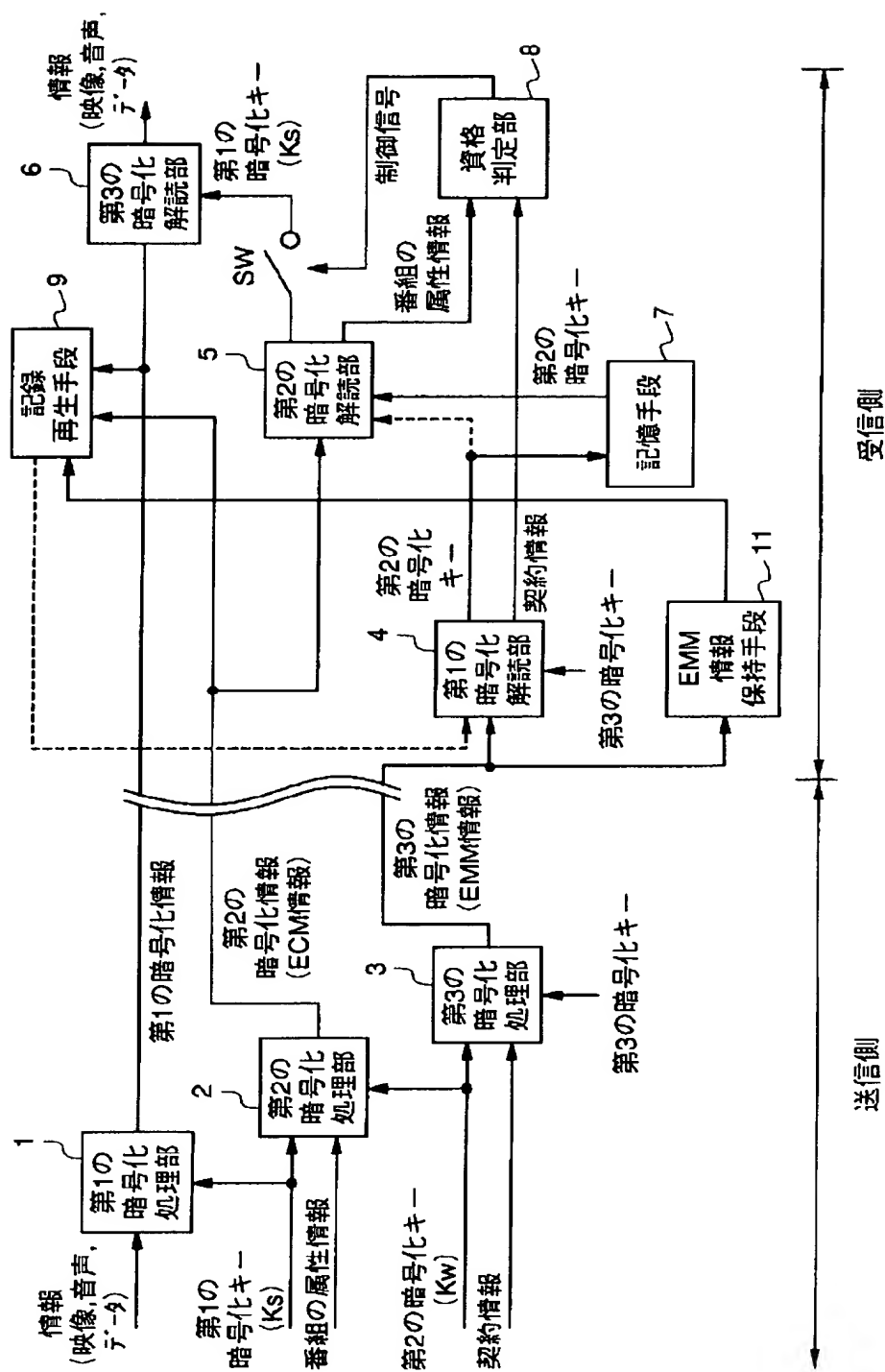
【図3】



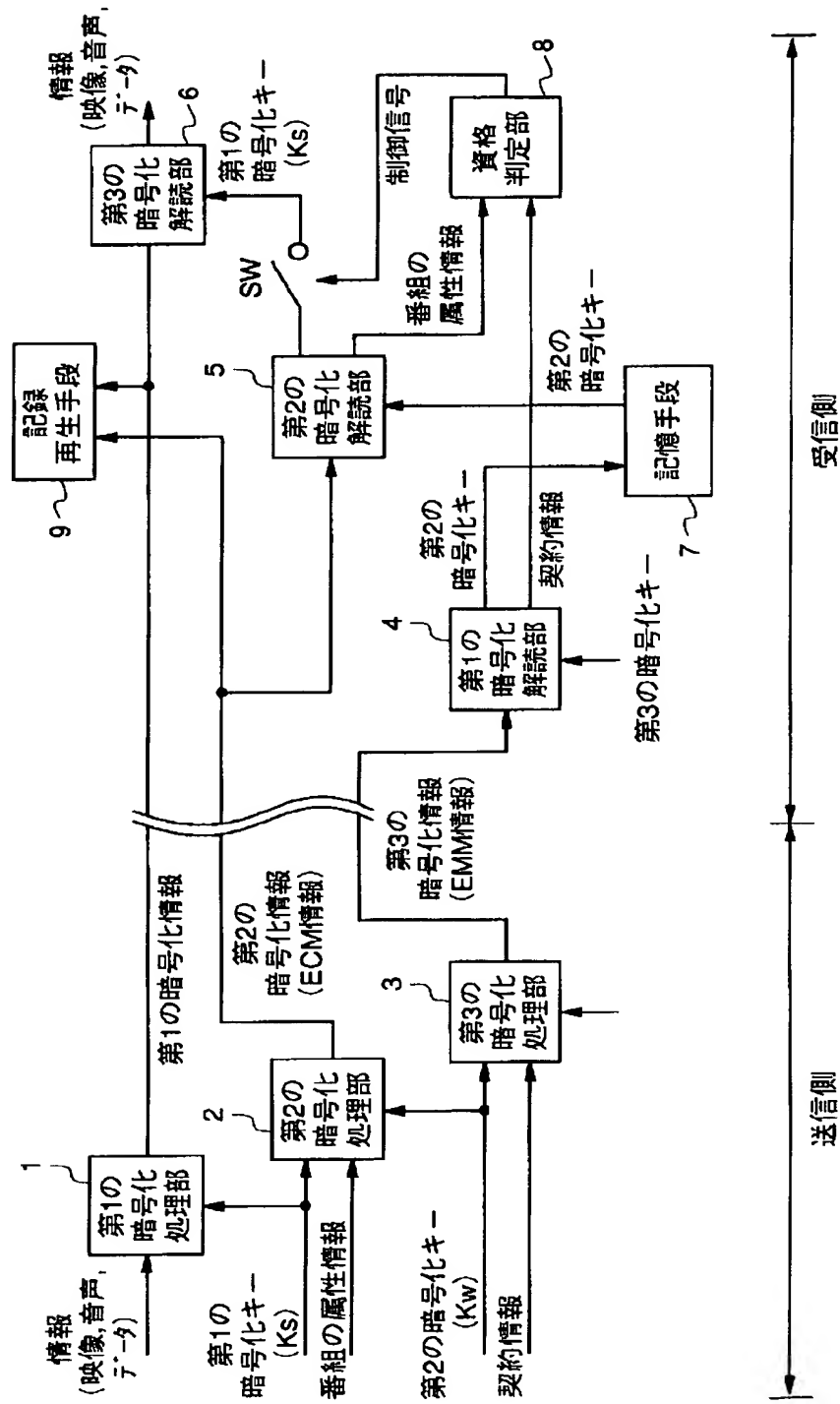
【図4】



【図 5】



【図7】



【図9】

